

REMARKS

Claims 1-22 are pending in the application. Claims 1, 10-16, and 18-22 have been amended. Applicant respectfully requests reconsideration of the pending claims in light of the amendments and the following remarks.

CLAIM OBJECTIONS

The Office Action objected to claims 1, 10, 16, and 19 for lack of antecedent basis. Applicant has amended the claims to correct the antecedent basis problem.

CLAIM REJECTIONS UNDER 35 USC §101

The Office Action rejected claims 11-16 under 35 USC 101 as being directed to non-statutory subject matter. Claim 11 has been amended to recite: “A computer readable storage medium comprising code that, when executed, causes a computer to perform the following.”

CLAIM REJECTIONS UNDER 35 USC §102

The Office Action rejected claims 11-12 and 14-16 under 35 USC 102(b) as being anticipated by Feldbaum (Patent No. 6,446,206 B1).

Claim 11 has been amended to recite the element of: “transmit the encrypted MQ message to a destination application program for processing of the data, wherein the source application program and the destination application program are separate by at least one

firewall.” Feldbaum does not teach or suggest the limitation wherein the two programs are separated by at least one firewall. See Office Action at page 8, item number 23: “Feldbaum doesn’t explicitly disclose for integrating applications hosted at different enterprises separated by at least one firewall.” Claim 11 is not anticipated by Feldbaum, therefore its rejection should be withdrawn.

Claims 12 and 14-16 are directly and indirectly dependent upon claim 1, therefore they are not anticipated by Feldbaum for at least the same reasons that claim 1 is not anticipated by Feldbaum.

The Office Action rejected claim 18 under 35 USC 102(e) as being anticipated by Smith (Patent No. 6,604,104 B1).

Claim 18 is not anticipated by Smith because the queue manager of Smith is not configured for receiving encrypted data. The last two elements of claim 18 state: “encrypting the MQ message using a security protocol to provide a secure MQ message; and transmitting the encrypted MQ message to a first queue manager for retransmission at a time when the network is suitable for transporting the message to the server.” Clearly, transmitting the encrypted MQ message to the queue manager is not taught or suggested by Smith, as stated in the Office Action at page 7, item number 18: “Smith doesn’t explicitly disclose that the queue manager receives encrypted data.” Therefore, the rejection to claim 18 should be withdrawn.

CLAIM REJECTIONS UNDER 35 USC §103

The Office Action rejected claims 1-4 under 35 USC 103(a) as being unpatentable over Smith in view of Chu et al. (Pub. No. 2002/0123966 A1). As stated in the Office Action at page 7, “Smith doesn’t explicitly disclose that the queue manager receives encrypted data.” Applicant submits that Chu does not disclose this element either. Chu guarantees a secure transmission of messages by only allowing authorized clients to access the message queue. Chu does not *transmit* encrypted messages; rather, Chu encrypts messages that are kept in the local queue. See Chu, at paragraph [0044]:

[0044] With respect to security, at the MSMQ message level, the transmission of messages from Client 82 to Server 80 is secure, since only an authorized Client 82 can access the message queue 98. Optionally, captured event messages can be encrypted while being kept in the local MSMQ queue 98, 95 on both Client 82 and Server 80 sites. Further, at the system level, using Virtual Private Network (VPN) with IPSec in a N-tier network environment enforces end-to-end identity authentication and data encryption. In addition, in regard to real time processing, a WMI NT log event is captured in real time as it occurs prior to the time the message content is written to the log and sent over to the Data Collector 80, immediately. This leaves absolutely no chance for data tampering at the Client site 82 under normal circumstance.

Therefore, claims 1-4 are not unpatentable over Smith in view of Chu because both of them fail to teach the required elements of the claimed subject matter as disclosed in claims 1-4.

The Office Action rejected claims 5-6, 8-10, 17 and 19 under 35 USC 103(a) as being unpatentable over Feldbaum in view of Butman (Patent No. 5, 867,665). As stated in the Office Action at page 8, “Feldbaum doesn’t explicitly disclose for integrating applications hosted at different enterprises separated by at least one firewall.” And further, as stated in the Office Action at page 10, “Feldbaum doesn’t explicitly disclose the target node is located at another side of a firewall from the agent.” The Office Action contends that Butman teaches “integrating applications hosted at different enterprises separated by at least one firewall” and cites FIG. 1a as support. Applicants traverss the finding of Butman as prior art. Butman does not teach a method with the capability to integrate applications across firewalls. As proof, Applicants submit Col. 13, line 66 – Col. 14, line 9 of Butman:

Still in FIG. 1a, client C2 might be an investment bank C2 that has offices in Hong Kong, New York and London, all connected with each other through the bank's wide area network C2WAN to form an internal network. The bank's entire network is shielded from external intrusion by firewall F2. Each of investment bank C2's sites at Hong Kong, New York and London has its own Local Area Network--C2-HKLAN in Hong Kong, C2-NYLAN in New York, and C2-LNLAN in London, with terminals T using standard commercially available Web browsers also connected at each Local Area Network.

As is apparent from reading the paragraph above, Butman’s firewall is external. The applications of Butman do not cross the firewall F2, they work completely within the firewall.

The Office Action rejected claim 13 under 35 USC 103(a) as being unpatentable over Feldbaum in view of Combar (US Patent Number 7,058,600 B1) (hereinafter “Combar”).

The Office Action at page 11 concedes that “Feldbaum doesn’t explicitly disclose the

computer readable medium further comprising an instruction for sending a message to the source application program instructing the source application program to stop sending data.” The Office Action contends, however, that Combar teaches this element.

Applicants disagree with this combination of references. Combar deals with viewing reports about customer’s telecommunication network traffic. Combar does not deal with messages transmitted via a message queuing protocol. Instead, Combar teaches: “After the predetermined period of time, e.g., seven days, the numbers scheduled for service deletion are passed to TVS via TCP/IP connectivity in real time. After receiving this information, TVS instructs the GSE 504 in real time to stop collecting CDRs for these numbers.” See Combar Col. 20, lines 20-25. Claim 13 is not unpatentable over Feldbaum in view of Combar.

The Office Action rejected claim 7 under 35 USC 103(a) as being unpatentable over Feldbaum in view of Butman and further in view of Combar (US 7,058,600 B1).

As stated in the Office Action at page 11, “As to claim 7, neither Feldbaum nor Butman explicitly disclose sending a message to the source application program instructing the source application program to stop sending data.” As Applicants previously stated, Combar does not teach this either; therefore, claim 7 is not unpatentable over Feldbaum in view of Butman and further in view of Combar.

The Office Action rejected claims 20-22 under 35 USC 103(a) as being unpatentable over Feldbaum in view of Butman and further in view of Smith.

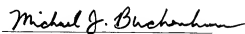
As stated in the Office Action at page 12, “As to claim 20, neither Feldbaum nor Butman explicitly discloses wherein transmitting the MQ message further comprises using a hypertext transfer protocol.” “As to claim 21, neither Feldman nor Butman explicitly discloses wherein transmitting the MQ message further comprises using a hypertext transfer protocol.” “As to claim 21, neither Feldbaum nor Butman explicitly discloses wherein transmitting the MQ message further comprises a secure socket layer protocol.” “As to claim 22, neither Feldbaum nor Butman explicitly discloses wherein transmitting the MQ message further comprises a hypertext transfer protocol over a secure socket layer.”

The Office Action further contends that it would have been obvious to modify the teachings of Feldbaum and Butman by transmitting the MQ message using a hypertext transfer protocol as taught by Smith “in order to support a web browser.” Office Action at page 12. Applicants traverse this finding and submit that the Examiner’s need to gather up multiple references in order to combine them is the very indicia of non-obviousness. If Feldbaum and Butman had the need for a hypertext transfer protocol “in order to support a web browser” and had the ability to configure their invention to do so, then they would have done so. Searching for multiple prior art references in order to re-engineer an invention is not in the spirit of the law. Indeed, any invention can be loosely construed as originating from multiple prior art references; this is why the Supreme Court has said: “As is clear from cases such *Adams* [383 U.S. 39(1966)], a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.” *KSR International Co., Petitioner v. Teleflex Inc., et al.*, 550 US ____ (2007), Supreme Court of the

United States, No. 04-1350:

For the foregoing reasons, Applicant respectfully requests allowance of the pending claims.

Respectfully submitted,

A handwritten signature in cursive script, reading "Michael J. Buchenhorner", is written over a horizontal line.

Michael J. Buchenhorner
Reg. No. 33,162

E-filed on Date: June 8, 2007

Michael Buchenhorner, P.A.
8540 S.W. 83 Street
Miami, Florida 33143
(305) 273-8007 (voice)
(305) 595-9579 (fax)